BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada zaman yang serba maju ini, teknologi telah masuk menjadi suatu bagian penting untuk manusia. Banyak sekali teknologi yang mampu membantu pekerjaan manusia pada era modern ini. Terlebih lagi pada saat pandemi COVID-19 kemarin, dimana kita dipaksa untuk tidak keluar rumah dan melakukan hampir segala aktivitas dirumah. Surel menjadi salah satu teknologi yang sering dan sangat membantu kita terutama dalam hal mengirimkan pesan penting atau file yang diperlukan kepada orang lain. Erima Oneta dan Yosep. S mengemukakan bahwa surel adalah salah satu fasilitas internet yang paling awal dikembangkan di internet. Surel juga dapat membantu kita dalam menyusun, mengirimkan, membaca, membalas, dan mengelola pesan secara elektronis dengan cepat, tepat, dan aman [1]. Kemudahan lain yang diberikan surel adalah surel tidak hanya dapat mengirimkan pesan berbasis tulisan ataupun file, tapi juga dapat mengirimkan pesan berbasis gambar. Jadi, kita sudah ingin mengirimkan gambar dengan resolusi yang tinggi dan tidak bisa dikirim melalui whatsapp atau platform komunikasi lain, email menjadi pilihan yang nyata bagi pengguna teknologi.

Disamping banyak kemudahan yang diberikan oleh surel, terdapat juga beberapa permasalahan yang sering menganggu penggunanya. Salah satu masalah yang kerap ditemui adalah *spam*. *Spam* juga disebut dengan *unsolicited bulk email* yang menyebabkan masalah komunikasi dalam penggunaan surel. *Spam* juga menempati sumber daya yang sangat besar, khususnya pada *bandwidth* jaringan dan ruang penyimpanan. Contoh kasus *spam* bisa berupa iklan perjudian, berita ataupun iklan yang tidak kita perlukan dan dapat menganggu kenyamanan kita dalam menggunakan surel[2]. Selain menganggu kenyamanan kita dalam menggunakan email, email spam juga sangat berbahaya karena email spam sering berisi konten berbahaya seperti *malware, virus* dan berita penipuan. Hal yang paling berbahaya dari surel *spam* adalah kebocoran data yang akhirnya dimanfaatkan oleh pihak-pihak yang tidak bertanggungjawab. Selain itu, sekarang sangat banyak

upaya penipuan yang dilakukan dengan cara surel *spam* tersebut, salah satu caranya adalah dengan menggunakan teknik manipulasi gambar. Cara kerja surel *spam* melalui gambar ini dilakukan dengan beberapa cara. Konten visual surel dapat disimpan di dalam file PNG ataupun JPG. Untuk melewati pemfilteran, penipu tersebut biasanya memanipulasi gambar dengan cara meregangkan gambar, mengubah warna, ataupun mengompresi gambar [3].

Surel *spam* ini menjadi suatu keresahan tersendiri untuk para pengguna surel di seluruh dunia. Per 18 Oktober 2021 di Amerika Serikat terdapat sekitar 8.61 miliar surel *spam*. Hal tersebut juga terjadi di negara China dengan sekitar 8,53 surel *spam* dan di negara India sebanyak 7,97 miliar surel *spam* [4]. Surel *spam* ini juga bisa mengarahkan kita kepada suatu web palsu sehingga dapat mengambil data pribadi korban. Selain itu, didalam spam juga terdapat malware yang berisikan *virus* yang berbahaya. Selain itu, dalam *spam* juga terdapat *scam*, yaitu penyamaran yang dilakukan dan bertujuan untuk mendapatkan simpati korban yang pada akhirnya pelaku bisa mendapatkan sesuatu hal yang dia inginkan seperti data maupun uang[5]. Surel *spam* juga memasuki babak baru, yaitu menggunakan gambar sebagai medianya. Surel *spam* berbasis gambar menjadi marak dilakukan karena kemungkinan untuk terdeksi oleh sistem semakin kecil, biasanya para pelaku mencoba memanipulasi gambar agar tidak mudah terdeteksi oleh sistem. Sebenarnya ada cara untuk menanggulangi hal tersebut, yaitu menggunakan metode *white-listed e-mail address*. *White-listed e-mail address* adalah pengelompokan alamat email yang sudah pasti terpercaya atau yang tidak akan mengirimkan surel *spam*. Tetapi, *white-listed e-mail address* juga mempunyai satu kelemahan, yaitu ketika ada pengirim baru yang mengirimkan surel berupa gambar, alamat email tersebut akan langsung terdeteksi sebagai *spammers*, karena tidak masuk kedalam *white-listed* tersebut [6]. Maka dari itu, penelitian mengenai bagaimana cara mengantisipasi surel *spam* berbasis gambar diperlukan. Yaitu untuk menanggulangi atau menciptakan sebuah metode baru yang lebih efisien untuk dilakukan agar kenyamanan dan keamanan data pribadi pengguna email tidak tersebar dan digunakan untuk hal-hal yang tidak semestinya.

Selain dengan menggunakan *white-listed email address* ada beberapa cara untuk mengklasifikasi atau bahkan mengatasi spam email tersebut dengan menggunakan algoritma Machine Learning, seperti Naive Bayes, Random Forest dan Support Vector Machine. Algoritma Naive Bayes adalah metode yang berguna untuk mengklasifikasikan. Algoritma ini memanfaatkan metode probabilitas dan statistik yang dicetuskan oleh Thomas Bayes, dengan cara memprediksi probabilitas dimasa depan berdasarkan pengalaman di masa yang lalu[7]. Selanjutnya ada metode Random Forest, yaitu suatu algoritma yang digunakan pada klasifikasi data dalam jumlah besar. Klasifikasi ini dilakukan menggunakan penggabungan pohon atau *decision tree* yaitu dengan melakukan training pada sampel data yang kita miliki. Penggunaan pohon yang semakin banyak akan mempengaruhi hasil menjadi lebih baik [8]. Terakhir ada metode Support Vector Machine. Metode tersebut adalah sebuah metode learning machine yang bekerja berdasarkan prinsip *Structural Risk Minimization* yang bertujuan menemukan *hyperlane* terbaik yang memisahkan dua buah *class* pada *input space* [9]. Dari penelitian-penelitian yang telah dilakukan sebelumnya, kebanyakan penelitian berfokus pada *text classification* untuk *email spam filtering*. Sistem spam filtering yang berfokus pada *text classification* memiliki celah yaitu, pengiriman email spam dengan bentuk gambar. Dengan celah ini, *attacker* atau *spammers* dapat mengirimkan spam email berbentuk *text-embedded image* untuk menghindari deteksi dari *email spam filtering* yang menggunakan *text classification filtering*.

1.2 Rumusan Masalah

Penelitian mengenai perbandingan algoritma deteksi surel spam umumnya hanya menggunakan *dataset* surel spam berbasis teks. Namun, dalam penelitian ini, peneliti melakukan perbandingan pada 3 model klasifikasi yaitu *Naïve Bayes*, *Support Vector Machine* dan *Random Forest* dengan menggunakan ekstraksi fitur N-gram untuk mendeteksi surel *spam* baik yang berbentuk teks maupun gambar. Dengan membandingkan parameter seperti akurasi, *False Positive Rate, Sensitivity, Specificity, Matthew Correlation Coefficient* dan hasil *confusion matrix* dari masing-masing model klasifikasi, maka dapat dirumuskan suatu masalah yaitu:

a. Bagaimana hasil pengujian pada setiap model klasifikasi yang digunakan dalam melakukan deteksi surel spam baik berbentuk teks dan gambar?
b. Model klasifikasi dan nilai N-gram manakah yang menunjukkan hasil klasifikasi terbaik?

1.3 Batasan Masalah

Pembatasan masalah bertujuan untuk lebih memfokuskan terhadap arah penelitah yang akan dilakukan. Batasan masalah sesuai dengan rumusan masalah yang diuraikan sebelumnya. Batasan dalam penelitin ini yaitu:

a. Penelitian hanya berlingkup pada perbandingan kinerja algoritma machine learning Naïve Bayes, Random Forest dan Support Vector Machine.
b. Penelitian ini berfokus pada deteksi surel *spam* berbasis teks dan gambar.
c. Penelitian ini hanya berlingkup pada deteksi surel *spam* berbahasa Inggris.
d. Penelitian ini menggunakan *tools* dengan Bahasa pemrograman Python yakni Google Collaboratory.
e. Penelitian ini menggunakan Bahasa pemrograman Python versi 3.10.11.
f. Penelitian ini menggunakan *open-source dataset* yang diambil dari *platform* Kaggle untuk surel *spam* dan SpamHunter untuk gambar *spam* yang disusun pada tahun 2004.
g. Penelitian menggunakan *library* Python Tesseract untuk ekstraksi teks dari gambar *spam*.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya secara teknis adalah untuk menambahkan ekstraksi fitur teks menggunakan Natural Language Processing dari surel *spam dataset* berbasis teks dan *dataset* gambar *spam* untuk kemudian dimodelkan menggunakan algoritma *machine learning* Naïve Bayes,

Random Forest, dan Support Vector Machine dan selanjutnya dilakukan evaluasi dari hasil pemodelan *machine learning*. Tujuan secara umum yang akan dicapai oleh peneliti dalam penelitiannya adalah untuk menghasilkan evaluasi penerapan algoritma *machine learning* tersebut dalam kaitannya dengan deteksi surel *spam* berbasis teks dan *text-embedded image spam*.

1.5 Manfaat Penelitian

Manfaat secara teoritis dari penelitian yang dilakukan peneliti adalah untuk mengetahui algoritma *machine learning* dengan tingkat akurasi tertinggi dalam pendeteksian surel *spam* dan *text-embedded image spam* sehingga dapat dijadikan sebuah referensi bagi penelitian berikutnya. Dalam segi pemanfaatan secara praktis, penelitian yang dilakukan peneliti ini dapat digunakan untuk penentuan algoritma yang sesuai untuk sistem deteksi surel *spam* maupun deteksi surel yang mengandung *text-embedded image spam*.

1.6 Sistematika Penulisan

Sistematika penulisan pada penelitian meliputi:

BAB I PENDAHULUAN. Bab ini berisi tentang latar belakang penulisan, rumusah masalah penelitian, batasan masalah penelitian, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA. Bab ini berisi tinjauan pustaka, dasar-dasar teori yang digunakan, perbandingan dan kajian terhadap penelitian sebelumnya yang relevan dengan topik penelitian.

BAB III METODE PENELITIAN. Bab ini berisi tentang metode penelitian yang mencakup jenis penelitian, metode pengumpulan data, metode pemodelan algoritma *machine learning*, pengujian data, metode evaluasi kinerja pemodelan *machine learning*, dan metode analisis.

BAB IV HASIL DAN PEMBAHASAN. Bab ini berisi tentang hasil dan pembahasan penelitian mengenai penerapan sistem dan implikasi penelitian.

BAB V PENUTUP. Bab ini berisi kumpulan dari hasil penelitian dan saran-saran

yang dibutuhkan untuk pengembangan sistem lebih lanjut di masa depan.